GB00
01354

The Patent Office

PCT/GB00/01354

09/980731

INVESTOR IN PEOPLE #2

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

4

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 03 MAY 2000

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference

Jg-2451

2. Patent application number
(The Patent Office will fill in this part)

9909590.3

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Telepathic Industries Ltd.,
37 Station Road,
London,
NW4 4PN,
United Kingdom.

Patents ADP number *(if you know it)*

7648165001

If the applicant is a corporate body, give the country/state of its incorporation

United Kingdom.

4. Title of the invention

Mechanism for securing reliable evidence from computers and listening devices.

5. Name of your agent *(if you have one)*

Graham Jones & Company

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

77 Beaconsfield Road,
Blackheath,
London,
SE3 7LG.

Patents ADP number *(if you know it)*

2097001 ✓

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description 5

Claim*(s)*

Abstract

Drawing*(s)* 1 +1 5

10. If you are also filing any of the following, state how many against each item.

Priority documents

Translations of priority documents

Statement of inventorship and right to grant of a patent *(Patents Form 7/77)* 2

Request for preliminary examination and search *(Patents Form 9/77)*

Request for substantive examination *(Patents Form 10/77)*

Any other documents *(please specify)*

11. I/We request the grant of a patent on the basis of this application.

Signature Graham Jones & Co Date 26/4/99

12. Name and daytime telephone number of person to contact in the United Kingdom
Mr G.H. Jones
0181 858-4039

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

Title:

Mechanism for securing reliable evidence from computers and listening devices

Technical Field

This invention relates to methods and apparatus for securing and preserving evidence from computers and listening devices in a form which eliminates or reduces the need for corroborative or supporting evidence regarding the circumstances of the making of the recording.

Background

Throughout the history of computing it has been known that evidence from computers has been modifiable in most cases without trace. Modification and fabrication of computer evidence has led to serious problems in the investigation and prosecution of computer crimes, in the management of computer security, in the keeping of business records in accordance with the security provisions of the Companies Acts and in the cost of litigation where evidence has been derived from computers.

In criminal investigations the reliability of evidence from computers has had to be secured by complex administrative procedures ("bagging and tagging") when freezing computer evidence at the scene of an alleged crime together with the use of image copying equipment to take bit image copies of suspected computer systems. Police officers and computer staff have had to give detailed evidence regarding how they secured computer systems and preserved the computer evidence. In managing computer security there have been cases where it has been difficult or impossible to show precisely what data or programs were on particular computer systems at particular
times. In the keeping of business records there have been concerns about the conversion of paper records into document image copies and their subsequent reliability as contemporaneous evidence. One security concern has been the fact that a document image copy can be used to create modified versions of itself which cannot be shown to be forgeries without a very expensive forensic examination being undertaken - and sometimes with it being impossible to prove that the document image is an unmodified original. Consequently expensive administrative controls regarding the storage of document image copies are necessary to maintain adequate security.

Additionally police and security services have made greater use of listening devices under warrant for the monitoring of suspected criminals. Currently under UK legislation the evidence from such listening devices can only be used for intelligence gathering purposes and cannot be tendered in evidence in civil or criminal trials. This situation is presently under review and it is anticipated that UK law will be changed to allow for evidence from listening devices under warrant to be admissible in civil and criminal trials in certain circumstances. Concern has been expressed regarding the need for security services personnel to testify regarding the planting of listening devices and their compliance with administrative procedures to secure the reliability of evidence from listening devices.

Object of the Invention

It is the object of the invention to provide a computer peripheral, termed the "DataFreeze", which will automatically secure evidence in a form which will be accepted as being electronically "bagged and tagged" - that is to say the evidence will be encapsulated in a form which establishes precisely when it was obtained and where it was obtained.

According to the invention there is provided a device for use in validating recorded digitised voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit accommodating means for identifying the date, time and serial number of the device and the private key of a Public key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on standard recording media having a header and an enciphered message, the recorded message being enciphered with the date, time and serial number of the device and the header containing the private key encrypted date, time and serial number used in the cipher process.

According to the invention there is provided a process for use in validating recorded digitised voice, video, telemetry or digital computer generated information or the like, in which the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header containing the private key encrypted date, time and serial number used in the enciphering process.

According to a feature of the invention the cipher process and encrypted header also include geophysical location information indicative of the actual location of the device making the validated recording.

The process of the invention may be performed by a computer program which may be supplied on a suitable carrier.

The equipment of the invention performs these operations in real-time without adding any significant delay to the recording of the data, without the need for a powerful encryption microprocessor and without the need for skilled personnel. Once the recording has been secured and encapsulated by the DataFreeze hardware the resulting disk, tape, electronic recording, magnetic recording or optical recording is re-playable on any conventional replay device for the replay of that type of media running special DataFreeze deciphering software. Consequently, in one possible implementation, a prosecuting authority could supply to an accused's lawyers with a CDROM produced by the arresting officers on a DataFreeze peripheral which was readable by the accused's lawyers on their conventional windows personal computer with the DataFreeze decryption/deciphering software running. No additional hardware would be required by the defence lawyers. The date, time, CURSOR location and serial number of the DataFreeze peripheral used to make the recording would however always be available to the defence in confirmation of when, where and on what equipment the data had been frozen by the police or security forces.

Outside of the police and security services a DataFreeze peripheral could be used as an archival storage device in banking and financial services or as a tachograph or other work monitoring device in medical and in health and safety applications.

Description of one embodiment of the invention

The manufacturer, DataFreeze, generates a Public Key encryption pair for each unit to be manufactured - the public key being published as an X500 Digital Certificate and the private key being kept secret. Each private key is built into a custom chip in a tamper-proof module. Inside a DataFreeze peripheral is the custom chip in a tamper-proof module which is connected to a standard recording device (eg A CDROM writer or a floppy disk drive). The custom chip contains a geophysical positioning system (in one implementation of the invention a CURSOR positioning system), a real-time clock and a unique serial number. The output from these three devices, in one possible implementation, is converted into a 512 bit number with the left portion containing the data and time (D), the middle containing the positioning system's location (the CURSOR location) (C) and the right hand portion containing the Serial Number (S).

Within the custom chip the 512 bit number is encrypted using the private key of the particular unit. The resulting encrypted stream is called "H-Data". Because the volume of data (512 bits) being encrypted by the private key is very small, the vulnerability of the data to cryptoanalysis to discover the private key is very low. To start a recording session the DataFreeze unit receives data from an external source (e.g. a computer or a listening device). The DataFreeze unit notes the "H-Data" and writes this to the recording media as a header to the recording, padding any spare space in the header with zeros.

The DataFreeze unit now takes the first block of data received from the external source. It performs three simple Caesar cipher operations on the block of data · e.g. Multiplying the block of data by the new date and time and adding the cursor location and the square of the serial number .

ie DataFreeze block =([Data]*D1) + C+(S*S)

For the next block of data it performs a different calculation · eg Multiplying the block of data by the CURSOR location, adding the square of the new date and time (which will have increased a defined amount during the writing of the first block) and adding the serial number.

ie DataFreeze block =([Data]*C) + (D2*D2)+S

For the next block of data it performs a different calculation · eg Multiplying the block of data by the square of the serial number, adding the square of the CURSOR location and adding the new date and time (which will have increased a defined amount during the writing of the second block).

ie $\text{DataFreeze block} =([\text{Data}]*S*S) + D3+C$

For the fourth block of data the DataFreeze peripheral would reverts to enciphering using the algorithm used for the first block of data.

ie $\text{DataFreeze block} =([\text{Data}]*D4) + C+S$

Further variations on this manipulation are possible. However particular care must be taken in selection of the manipulations to avoid floating point operations which are likely to introduce floating point precision errors in the calculation when this is performed on conventional microprocessors.

The objective of the DataFreeze enciphering is not to make the data cryptographically secure ie secret. Rather it is to freeze the data as recorded with the date and time when was recorded, the location where it was recorded and the unit on which it was recorded. For proof of no tampering it has to do this in real-time. The simple manipulations of data are performed in a few cycles of the microprocessor running on the DataFreeze peripheral and cause no material delay in the writing of the data.

To replay a DataFreeze recording on a standard replay device the computer controlling the device would run the DataFreeze decryption/deciphering software. This would read the "H-data" from the header and decrypt it using the DataFreeze public key, which would be published as an X500 digital certificate. Once the header had been decrypted the left, middle and right portions of the header would be stored in buffers and used as the seed data for a computer program to step through the obverse of the enciphering process. Thus in the suggested implementation the first block of DataFreeze data would be have the CURSOR location subtracted and the square of the serial number subtracted with the result being divided by the data and time.

ie $\text{Data} = ([\text{DataFreeze Data}] - C -(S*S))/D1$

The second block of DataFreeze data would have the square of the new date and time (which will have increased a defined amount during the writing of the first block) subtracted , the serial number subtracted and the result divided by the CURSOR location.

ie $\text{Data} = ([\text{DataFreeze Data}] - D2 -S)/C$

The third block of data would have the square of the CURSOR location subtracted, the new date and time (which will have increased a defined amount during the writing of the second block) subtracted and the result divided by the square of the serial number.

ie $\text{Data} = ([\text{DataFreeze Data}] - (C*C) -D3)/(S*S)$

Such simple mathematical processes would not lead to any material overhead in the outputting of the data. It would also be possible to 'fast forward' and "'reverse' along a DataFreeze recording by noting the block number from the header and cycling through to the predicted algorithm, date and time, CURSOR location and serial number.

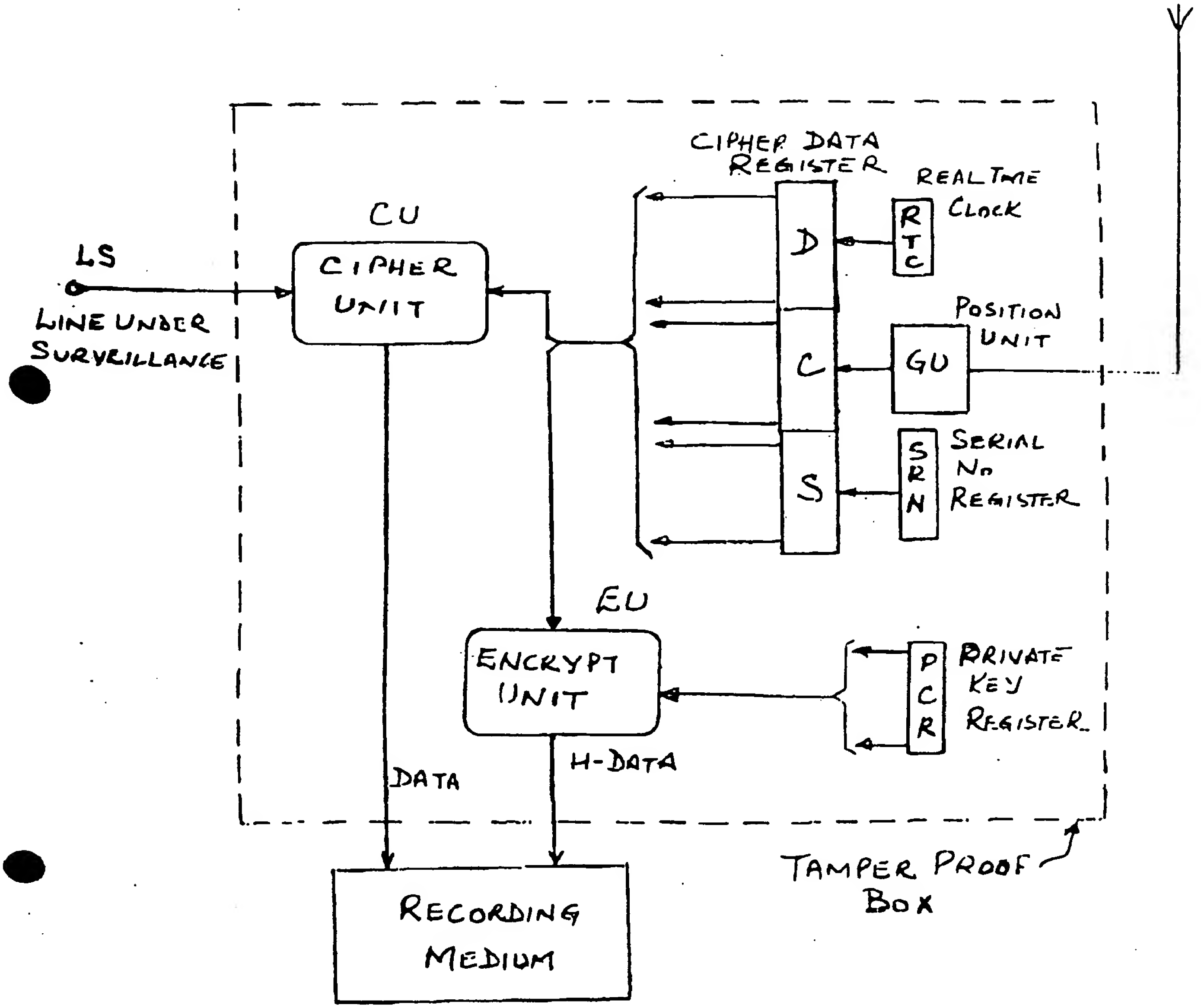
With sufficient computing power and time it would always be possible to decipher a DataFreeze recording which had lost its header by trying various combinations of date, location and serial number against the fragment of the recording However because the H-Data is digitally signed using the private key of the DataFreeze X500 digital certificate of the particular unit and the private key is located within a tamper proof module within the CURSOR unit along with the real time clock it would not be possible to create a fabricated DataFreeze recording which predated the original since this would require the forgery of the cryptographically secure H-data in the header.

A more sophisticated version of the invention could include a "digital fingerprint" in the header along with the H-Data. This would be produced by simultaneously passing a duplicate of the entire data session through a one-way algorithm while it was being written to disk to produce a unique value known as a message digest which would, in effect, be a "digital fingerprint" of the session. This message digest could then be encrypted by the DataFreeze unit's private key and written to the header field of the recording. When decrypted in software by using the Data Freeze unit's X500 public key this message digest could be used to confirm the integrity and coherence of the recording of the data session.

A further version of the invention could contain a dummy or non-functional CURSOR unit located in the tamper-proof module. This would not determine the location of the unit but would simply give out a default location for inclusion in the H-Data. The DataFreeze unit would thus only stamp the data with the time and specific unit and the default location. Such a unit would have two main uses: Use in situations where it was not possible to get a location signal and use in situations where the cost of the DataFreeze unit needed to be low and the location information was not considered to be important.

In yet a further version of the invention the geophysical information may be used to control the use of the recording equipment by having an inbuilt location identifier which is programmable and is used to prevent use of the recording equipment if it is located outside the geophysical area indicated by the inbuilt location identifier.

A device in accordance with the invention is shown solely by way of example on the accompanying drawing. The various parts of the device are described and connected as shown on the drawing.


CU
CIPHER UNIT
LS
LINE UNDER SURVEILLANCE
CIPHER DATA REGISTER
REAL TIME CLOCK
R T C
D
C
S
POSITION UNIT
GU
SERIAL No REGISTER
S R N
EU
ENCRYPT UNIT
P C R
PRIVATE KEY REGISTER
DATA
H-DATA
RECORDING MEDIUM
TAMPER PROOF BOX

PCT/GB00/01354

10-4-00.

Graham Jones & Co